

SSS:ADW

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
(1) FACEBOOK USER ID 1132805002;  
AND (2) FACEBOOK USER ID  
100011740475726, THAT IS STORED AT  
PREMISES CONTROLLED BY  
FACEBOOK INC.

**TO BE FILED UNDER SEAL**

**APPLICATION FOR A  
SEARCH WARRANT FOR  
INFORMATION IN  
POSSESSION OF A PROVIDER  
(FACEBOOK ACCOUNTS)**

Case No. 19-1141M

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Joshua Croft, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook user IDs that are stored at premises owned, maintained, controlled or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber(s) or customer(s) associated with the user IDs.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since December 2016. I am currently assigned to the Child Exploitation Investigations Unit. During my tenure with HSI, I have participated in

investigations targeting individuals involved in the receipt, distribution and possession of child pornography and have conducted physical and electronic surveillance, executed search warrants, reviewed and analyzed electronic devices, and interviewed witnesses. As part of my employment with HSI, I successfully completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both of which included instruction with respect to the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints, and other legal processes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (sexual exploitation of children), 2252 and 2252A (activities relating to material constituting or containing child pornography), and/or 2423 (travel with intent to engage in illicit sexual conduct) (collectively, the "SUBJECT OFFENSES") have been committed by TOM BLAHA. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

#### **PROBABLE CAUSE**

5. In or about November 2019, HSI received information from the National Center for Missing and Exploited Children ("NCMEC") indicating that a Facebook account belonging to an individual named TOM BLAHA ("BLAHA") had communicated with another Facebook

account belonging to an apparent minor located in the Philippines (the “Victim”), and that such communications reflected the apparent enticement of a minor to engage in sexual activity, travel from the United States to the Philippines to engage in sexual activity with a minor, and the creation and sale of child pornography. The information received from the NCMEC included details relating to the accounts such as user name, ID number, e-mail address and IP addresses used to access the Facebook accounts.

6. The account belonging to BLAHA has the unique user ID “1132805002” (the “BLAHA ACCOUNT”). The information received from the NCMEC indicates that the BLAHA ACCOUNT connected to the Internet from different locations within Long Island, New York on October 8, 2019 and October 9, 2019. The BLAHA ACCOUNT also connected to the Internet from Manila, Philippines on or about October 17, 2019. The BLAHA ACCOUNT is registered to an individual with a given username of “Tom Blaha,” a date of birth of April 1, 1956, and an e-mail address of tom\_blaha@msn.com.

7. The account belonging to the apparent minor located in the Philippines has the unique user ID “100011740475726” (the “Victim Account”). The information received from the NCMEC indicates that the Victim Account connected to the Internet from Manila, Philippines on November 25, 2019. The Victim Account is registered to an individual with a date of birth of May 5, 1999. However, based on the facts described below, there is reason to believe that the Victim is a minor.

8. Based on messages exchanged between the accounts, which the NCMEC received and then forwarded to HSI, it appears that BLAHA and the Victim had met in person and engaged in sexual activity at least once before September 20, 2019, in exchange for money. For example, on September 20, 2019, BLAHA called the Victim his “girlfriend” and said she was the

“World[']s best kisser.” The Victim responded that she “got [her] money baby thank you so much,” and BLAHA wrote back, “Your welcome my lover.”

9. On or about September 23, 2019, BLAHA and the Victim discussed the Victim creating sexually explicit videos to send to BLAHA in exchange for money. Specifically, the Victim wrote, “My sister has offer on me she said you want me to make 3 video[s] with vibrator. I agree with her but can you make 30k for that it[']s [hard] for me.” BLAHA wrote back, “Ok my love . . . Make me happy.” Based on my training and experience, I believe the reference to “30k” means 30,000 Philippine pesos, which are worth approximately \$600.

10. BLAHA appears to have traveled to the Philippines on or about October 17, 2019 to meet the Victim and engage in sexual activity. For example, on or about October 4, 2019, BLAHA wrote to the Victim that he loved and missed her, that he would see her in two weeks, and that he “want[s] to pet it.” Then, on or about October 17, 2019, the following exchange occurred:<sup>1</sup>

Victim Account:	hi baby is it ok if we resdule our meeting tomorrow because im busy on 19 to my school???
BLAHA ACCOUNT:	Can you send me a few mirror pictures in underwear?
BLAHA ACCOUNT:	Babe, 130,000 pesos without fuck or 200,000 pesos with fuck??
...	
Victim Account:	200 pesos can do everything baby but no sex baby pls in not ready yet...

---

<sup>1</sup> Verbatim exchanges described herein are comprised of excerpts from a longer message thread. Gaps between excerpts are denoted with ellipses.

BLAHA ACCOUNT:                      So you choose 130,000 pesos, everything but  
fuck, that's fine

...

BLAHA ACCOUNT:                      See you later lover!! Shave your pussy, ok?

11.      BLAHA appears to have left the Philippines the next day, and wrote to the Victim that he would come back in January. He also referred to sending money to the bank account of the Victim's sister for the benefit of the Victim, which may indicate that the Victim is not old enough to have her own bank account. Specifically, on or about October 18, 2019, the following exchange occurred:

BLAHA ACCOUNT:                      I promise to think of you everyday till I come  
back in January

Victim Account:                        me too baby and thank you a lot

Victim Account:                        baby when did i got my money hope you dont  
mind i need for my mom...

BLAHA Account:                        I can send to your sisters bank like last time, takes  
a few days for international processing

12.      Based on information and belief, the Victim is under the age of 18. On or about December 2, 2019, HSI agents reviewed the Victim Account, which is publicly accessible and contains a large number of photographs of a young female who is the apparent owner of the account – i.e., the Victim. Based on the physical appearance of the individual depicted in those photos, the Victim is well under the age of 18 and may be as young as 13 or 14. Furthermore, in certain of the photos, the Victim is wearing a school uniform that appears to be consistent with those often worn by students in middle school or high school.

13.      On or about December 5, 2019, HSI agents reviewed publicly accessible video clips posted by the Victim on Facebook and other social media platforms, showing the Victim in

classrooms or other school settings. In those videos, there are many children that appear to be between approximately 6 and 13 years of age. Both the Victim and those children are wearing similar uniforms in the videos.

14. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos and other information with other Facebook users, and sometimes with the general public.

15. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state and zip code), telephone numbers, screen names, websites and other personal identifiers. Facebook also assigns a user identification number to each account.

16. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events and birthdays.

17. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. In my training and experience, suspects in child exploitation cases sometimes adjust their Facebook privacy settings to conceal incriminating information from law enforcement.

18. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments and links that will typically be visible to anyone who can view the user’s profile.

19. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link

to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

20. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

21. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

22. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

23. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

24. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through



the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

25. Users may access Facebook on different types of digital devices, such as mobile phones or tablet computers. When a user accesses Facebook on the same digital device using more than one unique user ID, it is possible for Facebook to link all of the accounts associated with those user IDs by “machine cookie ID.” In other words, Facebook is able to identify discrete sets of unique accounts that have all accessed Facebook using the same digital device. Based on my training and experience, individuals who use social media such as Facebook to engage in the solicitation of child pornography or other child exploitative activity typically use multiple accounts to avoid detection by law enforcement. Therefore, information associated with presently unknown Facebook accounts, which are linked by machine cookie ID to known Facebook accounts suspected of being involved in child exploitative activity, can itself contain evidence of such conduct.

26. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender. A poke by one user to another is typically indicative of some sort of social relationship between the two users.

27. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user’s access or use of that application may appear on the user’s profile page. Based on my training and

experience in child exploitation investigations, suspects sometimes use Facebook apps, which sometimes themselves have internal messaging capability, to communicate with and solicit underage individuals.

28. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles and other items; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

29. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

30. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries or complaints from other users. Social networking providers like

Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

31. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity

may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information and other account information.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

34. Based on the forgoing, there is probable cause to believe that within the BLAHA ACCOUNT and the Victim Account, there exists evidence of violations of the SUBJECT OFFENSES. Accordingly, a search warrant for the BLAHA ACCOUNT and the Victim Account is requested.

35. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.


**REQUEST FOR SEALING**

37. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

  
\_\_\_\_\_  
JOSHUA CROFT  
Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me on December 6, 2019

  
\_\_\_\_\_  
HONORABLE SANKET J. BULSARA  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with (1) the Facebook account associated with user ID “1132805002”; and (2) the Facebook account associated with user ID “100011740475726,” that is stored at premises owned, maintained, controlled or operated by Facebook Inc. (“Facebook”), a social networking company headquartered in Menlo Park, California. For the avoidance of doubt, the property to be searched includes information associated with any and all accounts linked to user ID “1132805002” by machine cookie ID.

## **ATTACHMENT B**

### **Particular Things to Be Seized**

#### **I. Information to Be Disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID (or any accounts linked to user ID "1132805002" by machine cookie ID) listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them (including, to the extent available, all such photos and videos as originally uploaded, including EXIF data);
- (c) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers;

- future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;
- (d) All other records of communications and messages made by, received by or associated with the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
  - (e) All “check ins” and other location information;
  - (f) All IP logs, including all records of the IP addresses that logged into the account;
  - (g) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
  - (h) All past and present lists of friends created by the account;
  - (i) All records of Facebook searches performed by the account;
  - (j) The types of service used by the user;
  - (k) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
  - (l) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account; and
  - (m) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.



## **II. Information to Be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251 (sexual exploitation of children), 2252 and 2252A (activities relating to material constituting or containing child pornography), and/or 2423 (travel with intent to engage in illicit sexual conduct) (collectively, the “SUBJECT OFFENSES”) involving TOM BLAHA since January 1, 2019 to the present, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) The travel of any person into the United States or from the United States to a foreign country with the purpose of engaging in illicit sexual conduct, including, but not limited to, sexual conduct with an individual under the age of 18;
- (b) The production, distribution, receipt or possession of child pornography;
- (c) The persuasion, inducement, enticement or coercion of an individual under the age of 18 to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct;
- (d) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the SUBJECT OFFENSES under investigation and to the Facebook account owner;
- (e) Evidence indicating the Facebook account owner’s state of mind as it relates to the crime under investigation; and
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS  
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is \_\_\_\_\_. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature